Claims

[c1] A security system comprising:

a) an authentication element that receives a biometric characteristic from a user, the authentication element broadcasting an authorization signal in response to identifying the user; and

b) a device communicator in wireless communication with the authentication element and in electrical communication with a computing device, the device communicator permitting the user to access the computing device in response to receiving the authorization signal broadcasted by the authentication element.

[c2] The security system of claim 1 further comprising a sensor that is attached to at least one of the authentication element and the device communicator, the sensor generating a sensor signal that is related to a status of at least one of the authentication element, the device communicator, and the computing device.

[c3] The security system of claim 2 wherein the sensor comprises a motion sensor and the status of the at least one of the authentication element, the device communicator,

and the computing device is related to a motion of the device communicator.

[c4] The security system of claim 2 wherein the sensor comprises a proximity sensor and the status of the at least one of the authentication element, the device communicator, and the computing device is related to a distance between the authentication element and the computing device.

[c5] The security system of claim 2 wherein the sensor comprises a motion/proximity sensor and the status of the at least one of the authentication element, the device communicator, and the computing device is related to a motion of the device communicator and a distance between the authentication element and the computing device.

[c6] The security system of claim 2 wherein the sensor comprises a clock and the status of the at least one of the authentication element, the device communicator, and the computing device is related to a time interval between two predetermined events associated with at least one of the authentication element, the device communicator, and the computing device.

[c7] The security system of claim 1 wherein the biometric

characteristic is chosen from the group comprising a finger-print, a retinal scan, a voice-print, a DNA signature, a facial scan, body impedance, and a written signature.

[c8] The security system of claim 1 wherein the authentication element comprises an electronic circuit that is integrated into at least one of a computer, a cellular telephone, a personal digital assistant, and a pager.

[c9] The security system of claim 1 wherein the authentication element is bound to at least one of the device communicator and the computing device.

[c10] The security system of claim 1 wherein at least one of the authentication element, the device communicator, and the computing device further comprises an alarm that indicates a presence of an unauthorized user.

[c11] The security system of claim 10 wherein the alarm is chosen from the group comprising an audible alarm, a light, a distress beacon, a vibrator, and an electric shock device.

[c12] A security system comprising:

a) an authentication element that receives a biometric characteristic from a user, the authentication element broadcasting an authorization signal in response to identifying the user; and

b) a computing device in wireless communication with the authentication element, the computing device executing a software program in response to receiving the authorization signal broadcasted by the authentication element the software program permitting the user to access the computing device.

[c13] The security system of claim 12 wherein the software program comprises an interface/administration software program.

[c14] The security system of claim 12 wherein the authentication element is bound to the computing device.

[c15] The security system of claim 12 further comprising a sensor that is attached to the authentication element, the sensor generating a sensor signal that is related to a status of at least one of the authentication element and the computing device.

[c16] The security system of claim 12 wherein the biometric characteristic is chosen from the group comprising a finger-print, a retinal scan, a voice-print, a DNA signature, a facial scan, body impedance, and a written signature.

[c17] A method of authenticating a user to a computing device, the method comprising:

a) obtaining a biometric characteristic from a user

that identifies the user;

b) broadcasting an authorization signal that is related to the biometric characteristic;

c) receiving the authorization signal that is related to the biometric characteristic; and

d) permitting the user to access the computing device in response to receiving the authorization signal.

[c18] The method of claim 17 wherein the permitting the user to access the computing device provides the user physical access to a secured area.

[c19] The method of claim 17 wherein the permitting the user to access the computing device provides the user access to a computer network.

[c20] The method of claim 17 wherein the permitting the user to access the computing device provides the user access to secured data.

[c21] The method of claim 17 wherein the biometric characteristic is chosen from the group comprising a fingerprint, a retinal scan, a voice-print, a DNA signature, a facial scan, body impedance, and a written signature.

[c22] The method of claim 17 wherein the authorization signal is transmitted through at least one of a wireless communication system, a IR communication system, an optical

communication system and an acoustical communication system.

[c23] The method of claim 17 further comprising sensing a status of the computing device in response to the presence of the authorization signal.

[c24] The method of claim 23 wherein the status of the computing device is chosen from the group comprising a proximity of the user to the computing device, a motion of the computing device relative to the user, a receipt of a user credential, and a risk level assigned to the computing device.

[c25] The method of claim 17 further comprising sensing a status of the computing device in response to the absence of the authorization signal.

[c26] The method of claim 25 wherein the status of the computing device is chosen from the group comprising a proximity of the user to the computing device, a motion of the computing device relative to the user, a receipt of a user credential, and a risk level assigned to the computing device.

[c27] The method of claim 17 further comprising denying the user access to the computing device in response to an absence of the authorization signal.

[c28] The method of claim 17 further comprising securing the computing device in response to an absence of the authorization signal.

[c29] A security system comprising:

a) means for obtaining a biometric characteristic from a user that identifies the user;

b) means for broadcasting an authorization signal that is related to the biometric characteristic;

c) means for receiving the authorization signal that is related to the biometric characteristic; and

d) means for permitting the user to access the computing device in response to receiving the authorization signal.